FortiClient - Compliance Guide

Version 5.6

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTIGATE COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING SERVICES
http://www.fortinet.com/training

FORTIGUARD CENTER
http://www.fortiguard.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

November 22, 2017
FortiClient 5.6 Compliance Guide
04-560-460240-20171122

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-11-22	Initial release

Introduction

This document clarifies compliance when using FortiClient in the following configurations:

- FortiClient with FortiGate on page 7
- FortiClient with FortiGate and EMS on page 8

The document also describes the following scenarios, which do not support compliance:

- FortiClient with EMS (Primary Telemetry connection) on page 10
- FortiClient with EMS (Secondary Telemetry connection) on page 10

Terminology

The following clarifies the terminology used in this document.

Term	Definition
Managed mode	FortiClient used with FortiGate or EMS.
Integrated mode	FortiClient used with FortiGate and EMS. In this scenario, FortiClient connects FortiClient Telemetry to FortiOS and EMS.
Primary Telemetry connection	The following are primary Telemetry connections: • Connection between FortiClient and FortiOS when FortiClient is used with FortiGate. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and the user manually connects FortiClient Telemetry to EMS. See FortiClient with EMS (Primary Telemetry connection) on page 10.
Secondary Telemetry connection	The following are secondary Telemetry connections: • Connection between FortiClient and EMS when FortiClient is used with FortiGate and EMS. See FortiClient with FortiGate and EMS on page 8. • Connection between FortiClient and EMS when FortiClient is used without FortiGate and FortiClient is deployed using an installer created in EMS or gateway IP lists are used to connect FortiClient and EMS. See FortiClient with EMS (Secondary Telemetry connection) on page 10.
Endpoint	Computer or device where FortiClient is installed. An endpoint has Internet access and is running a supported operating system.
Connect FortiClient Telemetry	Establish connection between FortiClient and FortiGate or FortiClient and EMS. This is also referred to as registering FortiClient to FortiGate/EMS.

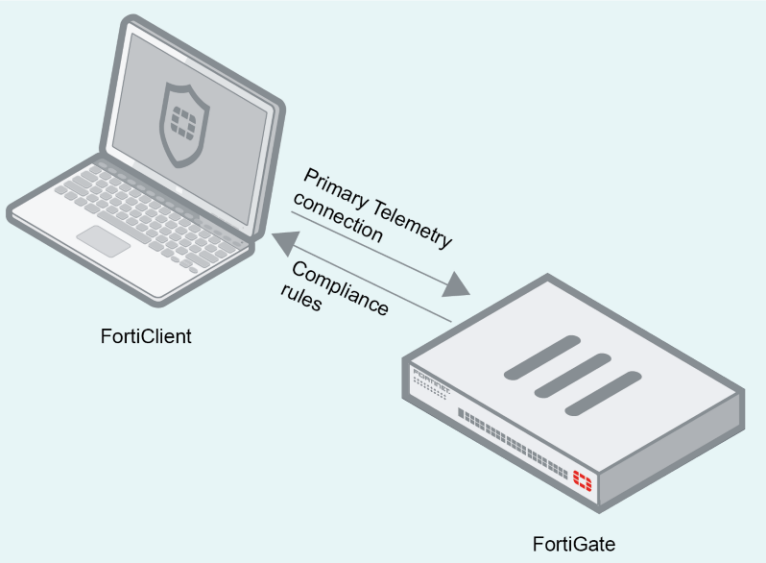
Term	Definition
Profile	XML configuration file provided from FortiGate or EMS to the endpoint when in managed or integrated mode. In FortiOS, administrators configure a *FortiClient Profile*. This profile defines compliance rules for endpoint access to the network through FortiGate. It also defines how FortiGate handles endpoints that fail to comply with compliance rules. In EMS, administrators configure an *endpoint profile*. This profile defines the configuration for FortiClient software on endpoints. Unless referring specifically to a profile created using FortiOS or EMS, this guide uses the term profile when referring to either a FortiClient Profile or an endpoint profile received by FortiClient.

Deployment Options for Compliance

This section describes the following deployment options: FortiClient with FortiGate and FortiClient with FortiGate and EMS.

FortiClient with FortiGate

In this scenario, FortiClient connects FortiClient Telemetry to FortiGate and compliance is supported. There is no connection to EMS.



FortiOS sends a FortiClient Profile to FortiClient. The FortiClient Profile includes compliance rules and some minimal configuration required to resolve non-compliance issues. The FortiClient Profile includes all compliance rules, whether enabled or disabled. FortiClient ignores disabled rules as they do not affect endpoint compliance.

You cannot configure FortiClient using FortiGate. To configure FortiClient, use EMS.

After receiving the FortiClient Profile, FortiClient compares its configuration with the compliance rules and reports to FortiOS which rules it is compliant with and which rules it is not compliant with. If the endpoint is not compliant, the following occurs depending on the FortiClient version number.

FortiClient 5.4.1 and later 5.4 versions

The following applies if the FortiClient version used is 5.4.1 and later 5.4 versions, and the FortiOS version used is 5.4.1 and later 5.4 versions.

If the compliance action is set to *block* in FortiOS, FortiClient blocks the endpoint's network access.

If the compliance action is set to *auto-update* in FortiOS 5.4.1, FortiClient auto-updates the configuration using the FortiClient Profile. If the endpoint is not compliant after updating, FortiClient blocks its network access.

If FortiClient is not compliant due to configuration issues, it can apply the FortiClient Profile. FortiClient only enables features (AntiVirus, Firewall, Web Filter, and so on) required by enabled compliance rules. Other features are not enforced so users can configure them as desired. A network administrator is not needed to enable such features.

FortiClient 5.6.0 and later 5.6 versions

The following applies if the FortiClient version used is 5.6.0 and later 5.6 versions, and the FortiOS version used is 5.6.0 and later 5.6 versions.

FortiClient does not block the endpoint's network access. FortiOS 5.6 makes the decision to block the endpoint's network access.

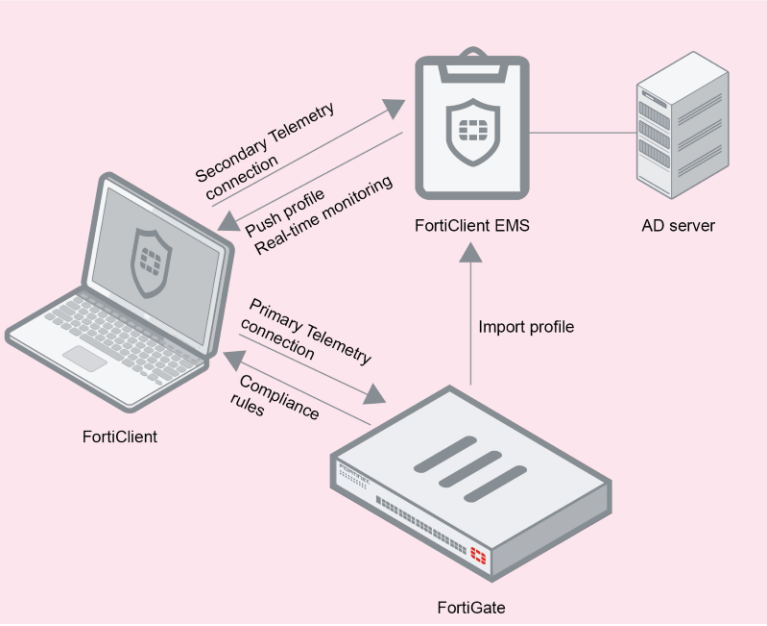
FortiOS blocks any endpoint where FortiClient is not installed or not connected to FortiOS. When FortiClient goes offline, it shows the compliance state, but the endpoint cannot access the Internet since FortiClient Telemetry is no longer connected.

If FortiClient is not compliant due to configuration issues, the user can change any configuration to make the endpoint compliant.

If allowed by configuration, FortiClient can be disconnected from FortiOS.

FortiClient with FortiGate and EMS

In this scenario, FortiClient establishes two FortiClient Telemetry connections: to FortiGate and to EMS. EMS pushes configuration information in an endpoint profile to FortiClient, while FortiOS provides compliance rules.



FortiClient follows the endpoint profile configuration received from EMS. FortiClient settings are locked so the endpoint user cannot change any configuration. EMS is expected to provide a profile that configures FortiClient to be compliant with rules received from FortiOS. If any configuration is not compliant, it must be fixed in EMS.

EMS can also import a FortiClient Profile from FortiOS and then push the profile to FortiClient.

In FortiClient Console, if allowed by the configuration, FortiClient can be disconnected from FortiOS. Disconnecting FortiClient from EMS can only be done in EMS.

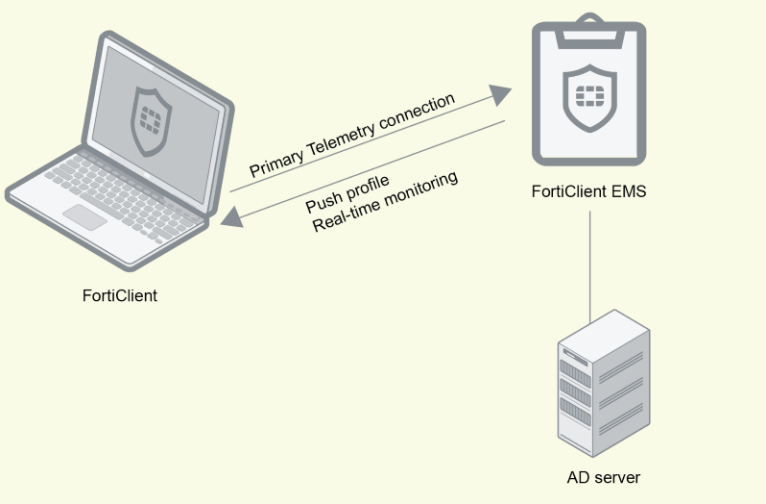
FortiClient installers created in EMS are embedded with the EMS server's IP address. This allows the endpoint to connect FortiClient Telemetry to the specified EMS server. The connection between FortiClient and EMS is a secondary Telemetry connection using a gateway IP list. See Secondary Telemetry connection on page 13.

Deployment Options without Compliance

This section describes the following deployment options: FortiClient with EMS only (primary Telemetry connection) and FortiClient with EMS only (secondary Telemetry connection).

FortiClient with EMS (Primary Telemetry connection)

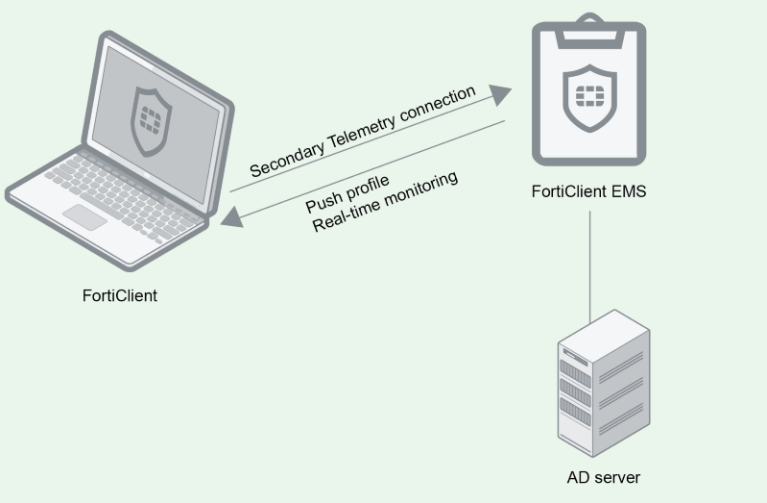
In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile from EMS. This scenario does not support compliance.



This scenario is possible if the user manually enters the EMS server's IP address in FortiClient Console.

FortiClient with EMS (Secondary Telemetry connection)

In this scenario, EMS provides FortiClient endpoint provisioning. FortiClient connects Telemetry to EMS to receive configuration information in an endpoint profile from EMS. This scenario does not support compliance.



This scenario is possible if FortiClient is deployed using an installer created in EMS or a gateway IP list is used to connect FortiClient and EMS. For details on how the secondary Telemetry connection differs from the primary Telemetry connection, see Secondary Telemetry connection on page 13.

How FortiClient Telemetry Connects to IP Addresses

FortiClient uses the following methods in the following order to locate FortiGate or EMS for Telemetry connection:

- Manual entering of the gateway IP address, which means that the endpoint user enters the gateway IP address of FortiGate or EMS into FortiClient Console.
- Telemetry Gateway IP list

  FortiClient Telemetry searches for IP addresses in its subnet in the gateway IP list. It connects to the FortiGate in the list that is also in the same subnet as the host system.

  If FortiClient cannot find any FortiGates in its subnet, it will attempt to connect to the first reachable FortiGate in the list, starting from the top. The order of the list is maintained as it was configured in the gateway IP list.
- Default gateway IP address

  The default gateway IP address is specified on the FortiClient endpoint and is used to automatically connect to FortiGate. This method does not support connection to EMS.

  FortiClient obtains the default gateway IP address from the operating system on the endpoint device. The default gateway IP address of the endpoint device should be the IP address for the FortiGate interface with Telemetry enabled.
- VPN
- Remembered gateway IP list

  You can configure FortiClient to remember gateway IP addresses when you connect Telemetry to FortiGate or EMS. Later FortiClient can use the remembered IP addresses to automatically connect Telemetry to FortiGate or EMS.

FortiClient uses the same process to connect Telemetry to FortiGate or EMS after the FortiClient endpoint reboots, rejoins the network, or encounters a network change.

Silent registration

When silent registration is enabled, FortiClient connects and reconnects Telemetry to FortiOS or EMS without notifying the user. The user is not required to confirm the connection.

By default, silent registration is enabled in endpoint profiles. As a result, when EMS is used to deploy FortiClient installers, silent registration is enabled. You can manually disable silent registration in EMS.

Reregistration

The EMS administrator can assign a gateway IP list to endpoints. Receiving the gateway IP list triggers FortiClient to connect to a server using the order above, even if FortiClient Telemetry is already connected to FortiOS or EMS.

Secondary Telemetry connection

Gateway IP lists contain the IP address of the EMS server where the gateway IP list was created. The secondary Telemetry connection uses the gateway IP list to connect FortiClient with the EMS server associated with that gateway IP list. The secondary Telemetry connection connects FortiClient with EMS in the following cases:

- FortiClient with FortiGate and EMS on page 8
- FortiClient with EMS (Secondary Telemetry connection) on page 10

Consider a situation where FortiClient has already established a secondary Telemetry connection to an EMS server. A user then attempts to establish a primary Telemetry connection between FortiClient and the same EMS server by entering the EMS server's IP address in FortiClient Console. In this case, FortiClient establishes the primary Telemetry connection and stops the secondary Telemetry connection. If the primary Telemetry connection stops or connects to FortiOS, the secondary Telemetry connection automatically resumes.

The secondary Telemetry connection is controlled by EMS and cannot be controlled from the endpoint.

The secondary Telemetry connection is identical to the primary Telemetry connection other than the following:

- There is no option to disconnect a secondary Telemetry connection in FortiClient.
- The Telemetry connection is online/offline only. On-net/off-net is not supported.